



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,909	12/21/2000	Sunil Podar	062891.0505	2621
5073	7590	01/24/2008	[REDACTED]	EXAMINER
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			[REDACTED]	MOORTHY, ARAVIND K
			ART UNIT	PAPER NUMBER
			2131	
			[REDACTED]	NOTIFICATION DATE
				DELIVERY MODE
			01/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

miv

Office Action Summary	Application No.	Applicant(s)	
	09/745,909	PODAR ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 09 November 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,2,4-17,19-32 and 34-49 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,2,4-17,19-32 and 34-49 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 21 December 2000 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application
	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. This is in response to the arguments filed on 9 November 2007.
2. Claims 1, 2, 4-17, 19-32 and 34-49 are pending in the application.
3. Claims 1, 2, 4-17, 19-32 and 34-49 have been rejected.
4. Claims 3, 18 and 33 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 2, 4-17, 19-32 and 34-49 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 1, 2, 4, 5, 13, 14, 16, 17, 19, 20, 28, 29, 31, 32, 34, 35, 43, 44, 46, 48 and 49 are rejected under 35 U.S.C. 102(b) as being anticipated by Dutta et al U.S. Patent No. 7,296,091.**

As to claim 1, Dutta et al discloses a method for authenticated access to multicast traffic, comprising:

receiving an Internet group management protocol at an access network router operable to authenticate a plurality of requests from a plurality of customer premise systems [column 22, lines 7-21], the received request identifying a user

requesting to join an IP multicast channel [column 14, lines 20-46], the IP multicast channel selected from a bundle of IP multicast channels offered for receipt by the user as a multicast package on a subscription basis [column 14, lines 47-67];

authenticating access privileges of the user to the multicast channel [column 18, lines 9-20]; and

disallowing the request in response to at least an unsuccessful authentication [column 18, lines 9-20].

As to claims 2, 17 and 32, Dutta et al discloses authenticating access privileges of the user comprises:

determining whether the user has access privileges to the multicast channel based on previously provisioned information for the user [column 18, lines 9-20]; and

unsuccessfully authenticating access privileges of the user to the multicast channel in response to at least the user not having access privileges to the multicast channel [column 18, lines 9-20].

As to claims 4, 19 and 34, Dutta et al discloses allowing the request in response to at least successful authentication [column 18, lines 9-20].

As to claims 5, 20 and 35, Dutta et al discloses that the multicast channel comprises at least one of video, audio, data and combinational content [column 18, lines 9-20].

As to claims 13, 28 and 43, Dutta et al discloses that the request is a subscriber join request [column 14, lines 20-46].

As to claims 14, 29 and 44, Dutta et al discloses that authenticating access privileges of the user comprises:

determining whether the multicast channel is a controlled access multicast channel [column 18, lines 9-20]; and
authenticating access privileges of the user to the multicast channel in response to at least the multicast channel comprising the controlled access multicast channel [column 18, lines 9-20].

As to claim 16, Dutta et al discloses a system for authenticated access to multicast traffic, comprising:

receiving an Internet group management protocol at an access network router operable to authenticate a plurality of requests from a plurality of customer premise systems [column 22, lines 7-21], the received request identifying a user requesting to join an IP multicast channel [column 14, lines 20-46], the IP multicast channel selected from a bundle of IP multicast channels offered for receipt by the user as a multicast package on a subscription basis [column 14, lines 47-67];

authenticating access privileges of the user to the multicast channel [column 18, lines 9-20]; and

disallowing the request in response to at least an unsuccessful authentication [column 18, lines 9-20].

As to claims 31, Dutta et al discloses a system for authenticated access to multicast traffic, comprising:

logic encoded in media [column 18, lines 9-20]; and
logic operable to receive and authenticate a plurality of requests received from a plurality of customer premise systems [column 22, lines 7-21], at least one of the plurality of requests comprising an Internet group management protocol request for a user to join an IP multicast channel selected from a bundle of IP multicast channels offered for receipt by the user as a multicast package on a subscription basis [column 14, lines 47-67], to authenticate access privileges of the user to the multicast channel and to disallow the request in response to at least an unsuccessful authentication [column 18, lines 9-20].

As to claim 46, Dutta et al discloses a method for providing premium content services over a network using Internet protocol (IP) multicast channels, comprising:

provisioning user access privileges to an IP multicast channel providing premium content, the premium content including at least one of video, audio and data [column 18, lines 9-20];

authenticating access privileges of a user to the IP multicast channel upon receiving an Internet group management protocol request at an access network router operable to authenticate a plurality of requests from a plurality of customer premise systems [column 22, lines 7-21], the received request identifying a user requesting to join the IP multicast channel to receive the premium video content,

the IP multicast channel selected from a bundle of IP multicast package on a subscription basis [column 14, lines 47-67]; and
disallowing the request in response to unsuccessful authentication [column 18, lines 9-20].

As to claim 48, Dutta et al discloses a method for authenticated access to multicast traffic, comprising:

receiving an Internet group management protocol request at an access network router operable to authenticate a plurality of requests received from a plurality of customer premise systems [column 22, lines 7-21], the received request identifying a user requesting to join an IP multicast channel [column 14, lines 20-46], the IP multicast channel selected from a bundle of IP multicast channels offered for receipt by the user as a multicast package on a subscription basis [column 14, lines 47-67];

authenticating access privileges of the user to the multicast channel [column 18, lines 9-20];

replicating multicast channel, at the access network router, in response to at least a successful authentication [column 18, lines 9-20]; and

transmitting the replicated multicast traffic to a customer premise system associated with the user [column 18, lines 9-20].

As to claim 49, Dutta et al discloses a method for authenticated access to multicast traffic, comprising:

receiving an Internet group management protocol request at an access network router operable to authenticate a plurality of request from a plurality of customer premise systems [column 22, lines 7-21], the received request identifying a user requesting to join a selected IP multicast channel [column 14, lines 20-46];

authenticating access privileges of the user to the multicast channel by determining if the selected IP multicast channel is within a bundle of IP multicast channels offered for receipt by the user as a multicast package on a subscription basis [column 18, lines 9-20]; and

disallowing the request in response to determining that the selected IP multicast channel is not within the bundle of IP multicast channels [column 18, lines 9-20].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 6, 7, 21, 22, 36 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 as applied to claims 1, 16 and 31 above, and further in view of Lloyd et al U.S. Patent No. 6,219,790 B1.

As to claims 6, 7, 21, 22, 36 and 37, Dutta et al does not teach prior to receiving the request, provisioning the user's access privileges in an authentication, authorization, and accounting (AAA) server. Dutta et al does not teach accessing the AAA server to authenticate access privileges of the user to the multicast channel. Dutta et al does not teach an AAA server that comprises a remote authentication dial-in user service (RADIUS) server.

Lloyd et al teaches provisioning a user's access privileges in an authentication, authorization, and accounting (AAA) server [column 4, lines 22-29]. Lloyd et al teaches accessing an AAA server to authenticate access privileges of a user [column 5, lines 33-41]. Lloyd et al teaches an AAA server that comprises a remote authentication dial-in user service (RADIUS) server [column 6, lines 49-53].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that there would have been an authentication, authorization, and accounting (AAA) server. The AAA server would have been

used to authenticate access privileges of the user to the multicast channel. The AAA server would have comprised a remote authentication dial-in user service (RADIUS) server.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Lloyd et al because the AAA server supports a variety of authentication transport protocols used by a variety of client types and is capable of supporting accounting functionality from the same database used to store user authentication and authorization information [column 2, lines 40-45].

8. Claims 8, 23 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 as applied to claims 1, 16 and 31 above, and further in view of Dynarski et al U.S. Patent No. 6,466,571 B1.

As to claims 8, 23 and 38, Dutta et al teaches that the multicast channel comprises an Internet protocol (IP) multicast channel, as discussed above.

Dutta et al does not teach that the request includes an IP address of the user device, further comprising determining the user based on the IP address of the device.

Dynarski et al teaches that the request includes an IP address of the user device. Dynarski et al teaches determining the user based on the IP address of the device [column 5, lines 36-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that the request would have included an IP address of the user device. The user would have been determined based on the IP address of the device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Dynarski et al because it ensures only authorized devices have access to the services available on the network.

9. Claims 9, 24 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 as applied to claims 1, 16 and 31 above, and further in view of Unitt et al U.S. Patent No. 6,718,387 B1.

As to claims 9, 24 and 39, Dutta et al does not teach determining whether the multicast channel comprises a public multicast channel. Dutta et al does not teach successfully authenticating access privileges of the user to the multicast channel in response to at least the multicast channel comprising the public multicast channel.

Dutta et al teaches determining whether the multicast channel comprises a public multicast channel. Dutta et al teaches successfully authenticating access privileges of the user to the multicast channel in response to at least the multicast channel comprising the public multicast channel [column 6 lines 9-44].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that it would have been determined whether the multicast channel comprised a public multicast channel. Access privileges would have been successfully authenticated of the user to the multicast channel in response to at least the multicast channel comprising the public multicast channel.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Dutta et al because this ensures that if the multicast is private a check is made to determine whether the join request

submitted is a duplicate of a previous request and thus prevents any unauthorized users to gain access with a duplicated request [column 6 lines 9-44].

10. Claims 10-12, 25-27 and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 as applied to claims 1, 16 and 31 above, and further in view of Ronen U.S. Patent No. 6,026,441.

As to claims 10-12, 25-27 and 40-42, Dutta et al does not teach determining whether the user is logged in to a service provider providing the multicast channel. Dutta et al does not teach unsuccessfully authenticating access privileges of the user to the multicast channel in response to at least the user not logged in to the service provider.

Ronen teaches determining whether the user is logged in to a service provider. Ronen teaches unsuccessfully authenticating access privileges of the user in response to at least the user not logged in to the service provider [column 2, lines 54-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that it would have been determined whether the user was logged in to a service provider that provided the multicast channel. The user would not have been successfully authenticated to access privileges if the user were not logged on to the service provider.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Ronen because by ensuring that the user is logged on and that it is a known user, it enhances security so that a third party does not try and intercept services.

11. Claims 15, 30 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 as applied to claims 1, 16 and 31 above, and further in view of Hooper et al U.S. Patent No. 5,671,225.

As to claims 15, 30 and 45, Dutta et al does not teach determining if authentication is enabled at an access router receiving the request. Dutta et al does not teach authenticating access privileges of the user to the multicast channel in response to at least determining that authentication is enabled at the router. Dutta et al does not teach allowing the request in response to at least determining authentication is not enabled.

Hooper et al teaches determining if authentication is enabled at an access router receiving the request. Hooper et al teaches authenticating access privileges of the user to the multicast channel in response to at least determining that authentication is enabled at the router. Hooper et al teaches allowing the request in response to at least determining authentication is not enabled [column 3, lines 33-42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that it would have been determined if authentication had been enabled at an access router receiving the request. Access privileges of the user to the multicast channel would have been authenticated in response to at least determining that authentication had been enabled at the router. The request would have been allowed in response to at least determining authentication has not been enabled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Hooper et al because by

doing authentication on a proxy (i.e. router) it reduces the chances of the service provider of getting attacked by a third party.

12. Claim 47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta et al U.S. Patent No. 7,296,091 in view of Ronen U.S. Patent No. 6,026,441.

As to claim 47, Dutta et al discloses receiving a request for a user to join an Internet protocol (IP) multicast channel, as discussed above. Dutta et al discloses authenticating access privileges of the user to the IP multicast channel by determining whether the IP multicast channel is a public multicast channel, as discussed above. Dutta et al discloses successfully authenticating access privileges of the user to the IP multicast channel in response to at least one of determining the multicast channel is a public multicast channel, as discussed above. Dutta et al discloses that that the multicast channel comprises an Internet protocol (IP) multicast channel and the request comprises an Internet group management protocol (IGMP) join request, as discussed above. Dutta et al discloses that the request is at an access network router operable to authenticate a plurality of requests from a plurality of customer premise systems, as discussed above.

Dutta et al does not teach determining that the user is logged in to the service provider and the service. Dutta et al does not teach unsuccessfully authenticating access privileges of the user to the IP multicast channel in response to at least one of determining the user is not logged in to the service provider and determining the user is not logged in to the service. Dutta et al does not teach terminating the request in response to at least an unsuccessful authentication. Dutta et al does not teach processing the request in response to at least a successful authentication.

Ronen teaches determining that the user is logged in to the service provider and the service. Ronen teaches unsuccessfully authenticating access privileges of the user to the IP multicast channel in response to at least one of determining the user is not logged in to the service provider and determining the user is not logged in to the service. Ronen teaches terminating the request in response to at least an unsuccessful authentication. Ronen teaches processing the request in response to at least a successful authentication [column 2, lines 54-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al so that it would have been determined whether the user was logged in to a service provider and the service. The request would have been terminated in response to at least an unsuccessful authentication. The request would have been processed in response to at least a successful authentication. The multicast channel would have comprised an Internet protocol (IP) multicast channel and the request would have comprised an Internet group management protocol (IGMP) join request.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dutta et al by the teaching of Ronen because by ensuring that the user is logged on and that it is a known user, it enhances security so that a third party does not try and intercept services.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
January 21, 2008

CHRISTOPHER REVAK
PRIMARY EXAMINER
CR